Indian J. pure appl. Math., 20 (2) : 99-103, February 1989

CYCLOTOMIC NUMBERS AND A CONJECTURE OF SNAPPER

S. A. KATRE

Department af Mathematics, S. P. College
Pune 411 030

(*Received* 23 *May* 1988)

The purpose of this note is to prove a conjecture of Snapper [*J. Algebra* 97 (1985), p. 277] by relating the numbers c_{ij} defined by him with cyclotomic numbers and using elementary properties of Jacobi sums.

1. INTRODUCTION

Let F_q be a finite field of q elements (q not necessarily a prime) and let γ be a generator of the cyclic group F_q^*. Let $e > 1$ be a divisor of $q-1$ and let ζ be a primitive (complex) eth root of unity. Let χ be the character on F_q defined by $\chi(\gamma) = \zeta$ and $\chi(0) = 0$. For i, j modulo e, the e^2 cyclotomic numbers A_{ij} and the e^2 Jacobi sums $J(i, j)$ of order e are defined by

$$A_{ij} = \text{Card. } \{v \in F_q \mid \chi(v) = \zeta^i, \chi(v+1) = \zeta^j\} \qquad \ldots(1.1)$$

and

$$J(i, j) = \sum_{v \in F_q} \chi^i(v)\, \chi^j(v+1). \qquad \ldots(1.2)$$

Let $q = 1 + ef$ and let H_f be the unique subgroup of F_q^* of order f. In other words H_f is the subgroup generated by γ^e. Snapper[3] defines an $e \times e$ matrix $C_e = (c_{ij})$ of nonnegative integers by

$$c_{ij} = \text{Card. } H_f \cap (\gamma^i + \gamma^j H_f) \qquad \ldots(1.3)$$

and conjectures that for fixed e,

$$c_{ij} \to \infty \text{ as } q \to \infty. \qquad \ldots(1.4)$$

(See conjecture 8.1 in Snapper[3]).

In section 2, we state some known properties of $J(i, j)$ indicating their proofs. In section 3, we obtain the asymptotic behaviour of the cyclotomic numbers A_{ij}. In section 4, we connect the numbers c_{ij} with A_{ij} and prove Snapper's conjecture. In section 5, we show that the c_{ij} and the A_{ij} of order e are positive for $q > e^4$ ($e > 1$), a result of interest in connection with Section 8 in Snapper[3].

2. Elementary Properties of Jacobi Sums

A relation between A_{ij} and $J(i, j)$ is given in

Lemma 1— $\sum_i \sum_j \zeta^{-(ai+bj)} J(i, j) = e^2 A_{ab}$.

The proof of this is similar to the proof of a particular case of this considered in, section 1 of Parnami *et al.*[2].

As in section 3 of Snapper[3]; define u to be the unique integer such that $-1 \in \gamma^u H_f$ and $0 \leqslant u \leqslant e-1$. Clearly $\chi^{(-1)} = \zeta^u$. By Proposition 3.2 of Snapper[3], if Char. $F_q = 2$, $u = 0$, If Char. $F_q > 2$, then if f is even $u = 0$; if f is odd, e is even and $u = e/2$. u may also be considered modulo e according to the context.

Lemma 2— $J(0, 0) = q-2$. For $i, j \not\equiv 0 \pmod e$, $J(i, 0) = -\zeta^{iu}$, $J(0, j) = J(i, -i) = -1$.

PROOF : $J(0, 0) = \sum_{v \in F_q - \{0, -1\}} 1 = q-2$

$$J(i, 0) = \sum_{v \neq -1} \chi^i(v) = -\chi^i(-1) = -\zeta^{iu}$$

$$J(0, j) = \sum_{v \neq 0} \chi^j(v+1) = -\chi^j(1) = -1.$$

$$J(i, -i) = \sum_v \chi^i(v)\chi^{-i}(v+1) = \sum_{v \neq -1} \chi^i\left(\frac{v}{v+1}\right)$$

$$= \sum_{v' \neq 1} \chi^i(v') = -\chi^i(1) = -1.$$

Lemma 3— $J(i, j)\,\overline{J(i, j)} = q$ for

$i, j, i+j \not\equiv 0 \pmod e$.

The proof of this lemma is similar to that of Lemma 1 of Parnami *et al.*[2].

3. The Asymptotic Behaviour of Cyclotomic Numbers

Let $X_{ij} = \{v \in F_q \mid \chi(v) = \zeta^i, \chi(v+1) = \zeta^j\}$, for i, j modulo e. Then $A_{ij} = \text{Card. } X_{ij}$. Clearly the X_{ij} are pairwise disjoint sets and $\bigcup_{i,j} X_{ij} = F_q - \{0-1\}$. Hence $\sum_i \sum_j A_{ij} = q-2$. The cyclotomic numbers of order e are e^2 is number and it is expected that the elements of $F_q - \{0, -1\}$ be almost equally distributed among the sets X_{ij} atleast for large q. This is confirmed by our following

Theorem 1— The cyclotomic numbers of order e are asymptotic to q/e^2 as $q \to \infty$. (In particular the cyclotomic numbers tend to ∞ along with q.)

PROOF : We have by Lemma 1,

$$e^2 A_{ab} = J(0,0) + \sum_{i=1}^{e-1} J(i,0)\,\zeta^{-ai} + \sum_{j=1}^{e-1} J(0,j)\,\zeta^{-bj} + \sum_{i=1}^{e-1} J(i,-i)\,\zeta^{-(a-b)i} + K \qquad \ldots (3.1)$$

where

$$K = \sum_{i,j,\, i+j \not\equiv 0 \pmod e} J(i,j)\,\zeta^{-(ai+bj)}.$$

By Lemma 2,

$$\begin{aligned} e^2 A_{ab} &= q-2 - \sum_{i=1}^{e-1} \zeta^{-(a-u)i} - \sum_{j=1}^{e-1} \zeta^{-bj} \\ &\quad - \sum_{i=1}^{e-1} \zeta^{-(a-b)i} + K \\ &= q-2 - (\epsilon(a-u) - 1) - (\epsilon(b) - 1) \\ &\quad - (\epsilon(a-b) - 1) + K \end{aligned}$$

where

$$\epsilon(a) = \begin{cases} e \text{ if } e \mid a, \\ 0 \text{ if } e \nmid a. \end{cases} \qquad \ldots (3.2)$$

Thus

$$e^2 A_{ab} = q + 1 - \epsilon(a-u) - \epsilon(b) - \epsilon(a-b) + K. \qquad \ldots (3.3)$$

Here,

$$|K| \leqslant \sum_{i,j,\, i+j \not\equiv 0 \pmod e} |J(i,j)| = (e-1)(e-2)\sqrt{q}. \qquad \ldots (3.4)$$

Dividing (3.3) by q and letting $q \to \infty$, we see that $e^2 A_{ab}/q \to 1$, i.e. A_{ab} is asymptotic to q/e^2 as required.

4. Proof of Snapper's Conjecture

We first connect the c_{ij} defined by Snapper (see (1.3)) with the cyclotomic numbers A_{ij} in the following :

Lemma 4— $A_{ij} = c_{i+u,j}$; $c_{ij} = A_{i+u,j}$.

Proof : $A_{ij} = \text{Card.} \left\{ v \in F_q^* \mid v \in \gamma^i H_f,\ v+1 \in \gamma^j H_f \right\}$

(*equation continued on p.* 102)

$$= \text{Card.} \left\{ v \in F_q^* \mid v\gamma^{-i} \in H_f, v\gamma^{-i} + \gamma^{-i} \epsilon \gamma^{-i+j} H_f \right\},$$

$$= \text{Card.} \left\{ v \in F_q^* \mid v\gamma^{-i} \in H_f, 1 \gamma^{-i} \epsilon - \gamma^{-i} + \gamma^{-i+j} H_f \right\},$$

$$= \text{Card.} \left\{ v' \in F_q^* \mid v' \in H_f, v' \epsilon - \gamma^{-i} + \gamma^{-i+j} H_f \right\},$$

$$= \text{Card. } H_f \cap (-\gamma^{-i} + \gamma^{-i+j} H_f),$$

$$= \text{Card. } H_f \cap (\gamma^{-j} + \gamma^{i-j} H_f) \text{ by Lemma 1.1 of Snapper}^3.$$

$$= c_{-j,i-j} = c_{j,i+u} = c_{i+u,j} \text{ (by Theorem 3.1 of Snapper}^3\text{).}$$

Hence

$$c_{ij} = A_{i+u,j} \text{ as } u \equiv -u \pmod{e}.$$

From Lemma 4 and our Theorem 1 we have :

Theorem 2— The entries c_{ij} of the matrix C_e are asymptotic to q/e^2 as $q \to \infty$.

In particular, we have, for fixed e,

$$c_{ij} \to \infty \quad \text{as} \quad q \to \infty \qquad \ldots(4.1)$$

proving the conjecture of Snapper.

5. A Remark

In Proposition 8.1 of Snapper[3] it is shown that certain Fermat-type equations have no nontrivial solutions in F_q (q a prime) or in integers, provided $c_{ij} = 0$. As we have shown that for fixed e, $c_{ij} \to \infty$ as $q \to \infty$, it may be interesting to see after what stage the c_{ij} (and so also the cyclotomic numbers) become positive.

From section 5 of Snapper[3], we see that the c_{ij} and the A_{ij} are positive for $e = 1$ when $q > 2$, and for $e = 2$ when $q > 5$. From (3.3) and (3.4) we get

$$e^2 A_{ab} \geqslant q + 1 - \epsilon(a-u) - \epsilon(b) - \epsilon(a-b) - (e-1)(e-2)\sqrt{q}. \qquad \ldots(5.1)$$

Here q is not necessarily a prime.

(Compare this with the result of Dickson[1] [45], viz. for $q = p$, a prime, and e an odd prime such that $p \equiv 1 \pmod{e}$,

$$e^2 A_{00} > p - 3e + 1 - (e-1)(e-2)\sqrt{p}.) \qquad \ldots(5.2)$$

From (5.1) we get, for all $i, j \pmod{e}$,

$$e^2 A_{ij} \geqslant q - (e-1)(e-2)\sqrt{q} - (3e-1). \qquad \ldots(5.3)$$

Now, for $x, b, c > 0$, we have,

$$x^2 - bx - c > 0 \text{ provided } x^2 > b^2 + 2c. \qquad \ldots(5.4)$$

Hence the right hand side of (5.3) is positive provided

$$q > (e-1)^2 (e-2)^2 + 2(3e-1). \qquad \ldots(5.5)$$

Therefore we have,

Proposition 1— The cyclotomic numbers A_{ij} and the numbers c_{ij} of order e are positive for

$$q > (e-1)^2 (e-2)^2 + 2(3e-1).$$

The right-hand side of (5.5) may be written as $e^4 - e(3e-2)(2e-3) + 2$. Hence for $e \geqslant 2$, the right-hand side of (5.5) is less than e^4. Thus we get a slightly weaker but interesting result viz.

Proposition 2— The A_{ij} and the c_{ij} of order e are positive for $q > e^4$ $(e > 1)$.

A result sharper than Propositions 1 and 2 but more awkward looking, which follows from (5.1), is

Proposition 3—The A_{ij} and c_{ij} of order e are positive when $q > \left(\frac{b + \sqrt{b^2+4c}}{2}\right)^2$ where $b = (e-1)(e-2)$ and $c = 3e-1$ or $2e-1$ according as $u = 0$ or $e/2$.

The bounds in these propositions can be sharpened to some extent for particular values of e using cyclotomy.

REFERENCES

1. L. E. Dickson, Cyclotomy and trinomial congruences, *Trans. Am. Math. Soc.* 37 (1935), 363-80.
2. J.C. Parnami, M. K. Agrawal and A. R. Rajwade, *Acta Arith.* 41 (1982), 1-13.
3. Ernst Snapper, *J. Algebra* 97 (1985), 267-77.